Goal: Provide CEOs with an understanding of the cyber threat environment with respect to the following

and to provide a brief update on cyber threat from

Introduction

(U) Good morning. I'm very pleased to be here again to provide you with a cyber threat update. For you to dedicate time at each of these meetings to cyber threat awareness really underlines for me that you see cyber security as critical to your business success.

(U) For us at the Communications Security Establishment, cyber security is our business. As the Government of Canada's centre of expertise on sophisticated cyber threats and defences, we're working with colleagues across the government to help protect Government of Canada networks and the information they contain.

(U) This includes supply chain integrity, engineering systems with security by design, and thwarting cyber-attacks.

(S) We view this as critical for Canada's national security, for government operations and for Canadians' privacy. In terms of a

metric to remember, CSE's advanced cyber defence capabilities are now blocking over 100 million probes of government systems each day.

(S) So the threat is real and is it growing – not just in terms of the number of attacks, but also the number and nature of threat actors and their motivations.

(U) We also understand how important cyber security is for Canada's economic security and for Canada's economic growth. We often refer to cyber security as a team sport but that makes it sound like fun; perhaps we should think of it more as a team imperative.

(U) In this spirit, CSE works with our partners in government, academia and the private sector to share expertise and knowledge so that you can better protect your systems and your information – whether it's your intellectual property, your critical business systems or your customers' personal and private information.

(S) Some of our key areas of focus in this domain are sharing of unique cyber threat information and intelligence, as well as working with industry to develop supply chain mitigation

frameworks. We are also focussing on creating ability for CSE to share our custom-developed cyber defence technologies and capabilities with the critical infrastructure sector.

(S) We are piloting some work

(S) And, CSE and Public Safety Canada

(U) We have been expanding our partnerships with the academic and technology community in Canada to kick start innovative cyber security research and expand the Canadian cyber security talent pool.

(U) That's a bit about us. Now, before I start with the briefing, I want to say that we have made an effort to be as open as possible and provide you with as much relevant information as we can.

(U) Much of this information is classified as SECRET, so we are asking you to treat it as such.

(S) In my previous briefing to this Council last August, I addressed the cyber threats - for example cyber-espionage - Canada faces, particularly from

(S) Today, I will provide a brief update on these as there have been notable developments over the past months.

(C) I'll then share cyber-threat information about

I'll leave some time for discussion at the end.

(C) As usual, we'll start with

(S)

(S) Last year I spoke about the state-sponsored theft of private sector intellectual property and proprietary business information,

Pages 5 to / à 8

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 15(1) - DEF, 15(1) - IA

of the Access to Information

de la Loi sur l'accès à l'information

(C) Now let me turn to an update on

Pages 10 to / à 14

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

I'll move on to another

Pages 16 to / à 25

are withheld pursuant to sections

sont retenues en vertu des articles

16(2)(c), 15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

(U) **Mitigation Strategies**

(U) Now that we've looked at the threats posed by what can governments and corporations do to better protect secrets, proprietary information and intellectual property?

(U) There are well-established best practices to follow that reduce risks and are applicable to most security contexts.

(U) For example, CSE's has created its Top Ten" IT security actions – a list of 10 things that Government of Canada departments can do to better protect its systems. While they are written for government, there are applications for you.

(U) There are other industry best practices such as the SANS Top 20 Security Controls. If implemented correctly, they can lead towards a solid baseline cyber security posture.

(U) When travelling outside Canada, CSE provides guidance to those traveling on government business in our IT Security Bulletins. This advice holds for the private sector as well.

(C) But as I've mentioned, doing business in foreign countries increases the threat that Canadian communications and data will

be monitored

(U) So the Government of Canada and Canadian corporations with global operations need to take this into account when considering where to store sensitive data and proprietary information, and in business practices when traveling or operating abroad.

(C) No doubt, this includes considering the duty of care associated with customer data, intellectual property and personal information, and the risks associated with current practices such as outsourcing IT security, cloud data storage, and the flow of data across global networks.

(C) As I've described, these risks are situationally-dependent and linked with a company's profile and the sectors in which it operates.

Conclusion

(U) I am going to wrap up here to give us time for discussion.

(U) I hope the briefing today gave you additional insight into the threat represented by

(U) I would expect that as the months and years go by, we will see an increasing number of countries developing and using cyber power.

(U) Canada and our allies will remain diligent in spotting and meeting these threats head on.

(U) I also hope that you'll leave with a better understanding of CSE's work. Together with Public Safety Canada and CSIS, we will continue to work to address cyber security issues that are relevant to Canada.

(U) We want to share information that is usable, that is delivered quickly and automatically, and that is relevant to cyber threats targeting Canadian businesses.

(U) We also want to expand our partnerships, and work more closely with you and academia, particularly in cyber R&D. Cyber security is a team sport.

(U) Thank you for the opportunity to talk to you today, and I look forward to working with you as we collectively protect one of Canada's most important resources – its information and intellectual property.